ABSTRACT

The present invention leverages the invertibility of determinants of unimodular matrices to provide a universal hash function means with reversible properties and high speed performance. This provides, in one instance of the present invention, length controllable hash values comprised of vector pairs that can be processed as one instruction in a SIMD (single instruction, multiple data) equipped computational processor, where the vector pair is treated as a double word. The characteristics of the present invention permit its utilization in streaming cipher applications by providing key data to seed the ciphering process. Additionally, the present invention can utilize smaller key lengths than comparable mechanisms *via* inter-block chaining, can be utilized to double hash values *via* performing independent hash processes in parallel, and can be employed in applications, such as data integrity schemes, that require its unique processing characteristics.